AMENDMENTS TO THE CLAIMS

The following is a complete listing of revised claims with a status identifier in parenthesis.

LISTING OF CLAIMS

What is claimed is:

1. (Currently Amended) A method wherein users are assigned a data key the method ~~for at least one of encrypting and decrypting data,~~ comprising:

performing a security check to ascertain an identity of a user;

associating the user with a user group including a plurality of users such that ~~assigning~~ a data key is assigned to the user based on the user group with which the user is associated, the data key being unviewable by the user, and the data key being for at least one of encrypting and decrypting data,~~ and being assigned on the basis of a result of the security check, wherein~~ the same data key [[is]] being assignable to [[a]] the plurality of users.

2. (Original) The method as claimed in claim 1, wherein the security check involves checking biometric data of the user.

3. (Original) The method as claimed in claim 1, wherein the security check involves checking a user-specific at least one of electronic and mechanical key.

4. (Original) The method as claimed in claim 1, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

5. (Original) The method as claimed in claim 4, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

6. (Original) The method as claimed in claim 1, wherein a plurality of data keys are simultaneously assignable to one user.

7. (Original) The method as claimed in claim 1, wherein the data are medically relevant, wherein the users include personnel at a medical facility, and wherein common user groups are assigned the same data key.

8. (Currently Amended) An electronic data processing facility ~~for at least one of encryption and decryption of data, wherein a data key for encrypting and decrypting data is assignable to a user,~~ comprising:

security check means for performing a security check to ascertain an identity of the user; [[and]]

means for associating the user with a user group including a plurality of users, the user being associated with the user group such that ~~means for assigning~~ a data key is assigned to the user based on the user group with which the user is associated, the data key being unviewable by the user, and the data key being for at least one of encrypting and decrypting data, ~~being assigned on the basis of a result of the security check, wherein~~ the same data key [[is]] being assignable to ~~various~~ the plurality of users.

9. (Original) The electronic data processing facility as claimed in claim 8, wherein the security check means is for checking biometric data from the user.

10. (Original) The electronic data processing facility as claimed in claim 8, wherein the security check means is for checking a user-specific at least one of electronic and mechanical key.

11. (Original) The electronic data processing facility as claimed in claim 9, wherein a data key memory is accessible by the data processing facility, for ascertaining the data key assigned by comparing the data obtained through the security check with the content of the data key memory.

12. (Original) The electronic data processing facility as claimed in claim 11, wherein the data key memory is arranged remotely from the data processing facility, and wherein the data processing facility uses a data telecommunication device to access the data key memory.

13. (Original) The electronic data processing facility as claimed in claim 8, wherein the data processing facility is a medical workstation for handling medically relevant data.

14. (Original) A storage medium, adapted to store information and adapted to interact with a data processing facility in order to carry out the method as claimed in claim 1.

15. (Original) The method as claimed in claim 2, wherein the security check involves checking a user-specific at least one of electronic and mechanical key.

16. (Original) The method as claimed in claim 2, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

17. (Original) The method as claimed in claim 3, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

18. (Original) The method as claimed in claim 16, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

19. (Original) The method as claimed in claim 17, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

20. (Original) The electronic data processing facility as claimed in claim 9, wherein the security check means is for checking a user-specific at least one of electronic and mechanical key.

21. (Original) The electronic data processing facility as claimed in claim 10, wherein a data key memory is accessible by the data processing facility, for ascertaining the data key assigned by comparing the data obtained through the security check with the content of the data key memory.

22. (Currently Amended) A method for at least one of encryption and decryption of data, comprising:

performing a security check to ascertain an identity of a user;

associating the user with a user group including a plurality of users such that ~~assigning a user~~ a data key for at least one of encrypting and decrypting data is assigned to the user based on the group with which the user is associated, the same data key being assignable to the plurality of users; and

~~performing a security check to ascertain an identity of a user~~

at least one of encrypting or decrypting data using the assigned data key~~, wherein a data key, unviewable by the user, is assigned to the user on the basis of a result of the security check, and wherein the same data key is assignable to a plurality of users~~.

23. (Original) A storage medium, adapted to store information and adapted to interact with a data processing facility in order to carry out the method as claimed in claim 22.

24. (Original) The method as claimed in claim 22, wherein the security check involves checking biometric data of the user.

25. (Original) The method as claimed in claim 22, wherein the security check involves checking a user-specific at least one of electronic and mechanical key.

26. (Original) The method as claimed in claim 22, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

27. (Original) The method as claimed in claim 26, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

28. (Original) The method as claimed in claim 22, wherein a plurality of data keys are simultaneously assignable to one user.

29. (Original) The method as claimed in claim 22, wherein the data are medically relevant, wherein the users include personnel at a medical facility, and wherein common user groups are assigned the same data key.

30. (Original) The method of claim 22, wherein users associated with a common user group are assigned the same data key.

31. (Currently Amended) An electronic data processing facility for at least one of encryption and decryption of data, comprising:

means for performing a security check to ascertain an identity of a user;

means for associating the user with a user group including a plurality of users ~~means for assigning~~ a data key is assigned to [[a]] the user based on the group with which the user is associated, the same data key being assignable to the plurality of users, and the data key being for at least one of encrypting and decrypting data; and

means for encrypting or decrypting data using the assigned data key

~~means for performing a security check to ascertain an identity of a user, wherein a data key, unviewable by the user, is assignable on the basis of a result of the security check, and wherein the same data key is assignable to a plurality of users~~.

32. (Original) The method of claim 1, wherein users associated with a common user group are assigned the same data key.